GESTION DE LA SÉCURITÉ

Énoncé repris

« Gérer la sécurité c'est aussi responsabiliser l'ensemble des acteurs sur le SI de l'entreprise. La sécurité ne se délègue pas. »

Sujet 02c : Gérer l'accueil en sécurité et la sensibilisation

Enseignant

Jacky Lemée

Équipe

Équipe 102

Membres

BEN BEKKOU Lynda
CONDETTE Jérémy
IBEROUALENE Melissa
KACED Inès
NIRERE Flavia

Année académique : 2025–2026

SOMMAIRE

1. Contexte et objectifs

➢ Contexte

Veridia est une entreprise qui vend un logiciel RH en ligne (paie, congés, notes de frais) à d'autres sociétés. Elle compte environ 300 employés, recrute souvent (CDI, alternants, prestataires) et travaille en hybride (bureau + télétravail). Veridia traite des données personnelles sensibles de ses clients, donc elle doit prouver qu'elle forme bien les nouveaux arrivants et qu'elle contrôle les accès.

➢ Outils du quotidien

- Messagerie et documents : Microsoft 365 (Outlook, OneDrive/SharePoint) ou Google Workspace (Gmail, Drive).
- Communication : Teams.
- Suivi de tâches et documentation : Jira.
- Code et dépôts : GitLab.
- Protection des postes : antivirus standard, mises à jour automatiques
- Connexions : compte unique pour tous les outils et double vérification à la connexion (mot de passe + code sur téléphone).

➢ Principaux risques à couvrir

Les incidents les plus probables chez Veridia sont simples et connus :

- Erreur humaine (e-mail piégé, lien douteux, pièce jointe dangereuse) -> fuite de données ou compte bloqué.
- Accès trop larges à l'arrivée (ou non retirés au départ) -> consultation ou action non autorisée.
- Perte/vol d'un ordinateur ou d'un téléphone -> exposition de fichiers ou d'e-mails.
- Partage de documents mal réglé.

Ces risques ont d'abord un coût très concret : temps perdu à rechercher des fichiers mal partagés, comptes bloqués, demandes clients pour "prouver" nos pratiques, il s'agit de protéger la confidentialité, garantir l'intégrité et d'assurer la disponibilité, conformément au RGPD (sécurité des traitements) et aux bonnes pratiques ISO/IEC 27001-27002.

➢ Objectifs du travail

1. Décrire un accueil en sécurité clair :

- ce qu'on fait avant l'arrivée,
- le Jour J et la Semaine 1.
- puis des rappels à 30 / 60 / 90 jours.

2. Mettre en place une sensibilisation obligatoire et courte.
3. Faire signer la charte informatique.
4. Clarifier qui fait quoi : RH, manager, équipe informatique, référent sécurité.
5. Suivre quelques indicateurs simples : taux de formation terminée, score moyen au quiz.

2. Méthodes et organisations

2.1 Démarche suivie

Nous avons travaillé de façon simple et cadrée, en 6 étapes :

➢ **Prise d'infos**

- Relecture de l'énoncé pour confirmer le périmètre (accueil en sécurité + sensibilisation) et pour choisir le contexte.

- Liste des livrables attendus : processus d'accueil, contenus de sensibilisation, indicateurs, preuves.

➢ **Récolte des besoins "métier"**

- Ce qu'attendent RH, manager, informatique et référent sécurité lors d'une arrivée.

- Contraintes simples à respecter : télétravail, outils courants (Teams, Jira, GitLab), traçabilité.

2.2 Répartition des tâches (qui a fait quoi)

- **BEN BEKKOU Lynda**
  Section 1 : Contexte, risques, objectifs, méthodes et organisations
- **IBEROUALENE Melissa**
  Section 3 : Accueil en sécurité (processus)
- **CONDETTE Jérémy**
  Section 4 : Sensibilisation et conformité
- **KACED Inès**
  Section 5 : Outils/indicateurs et amélioration continue
- **NIRERE Flavia**
  Section 6 :Recommandations

3. Accueil en sécurité (processus)

Le **processus d'accueil sécurité** de Veridia s'inscrit dans une démarche de **management par les processus (BPM)**.
Il transforme une **demande de recrutement** en un **collaborateur formé, équipé, habilité et conforme** aux exigences **RGPD** et **ISO/IEC 27001**.

Il a pour finalité de :

- garantir la **sécurité des accès et des données** dès l'intégration,
- réduire les **risques humains et techniques** liés à l'onboarding,
- fournir des **preuves de conformité** (RGPD, Code du travail, ISO 27001).

Le processus s'articule autour de trois grandes étapes :

- **préparation avant l'arrivée** (comptes, équipements, formations, tuteur),
- **accueil sécurité et prise en main des outils**,
- **suivi 30/60/90 jours** (droits d'accès, formations, pratiques) avec **archivage des preuves**.

Il s'appuie sur :

- des **outils** (Microsoft 365/Google Workspace, Teams, Jira, GitLab, SSO + MFA),
- des **acteurs identifiés** (RH, Manager N+1, IT, Sécurité/RSSI, Tuteur, collaborateur),
- une **checklist d'onboarding sécurité** complétée par le N+1 de l'« avant l'arrivée » à J+90,
- quelques **indicateurs simples** (% comptes créés avant J0, % collaborateurs formés sous 7 jours, incidents liés aux accès).

Les résultats (indicateurs, audits, incidents, retours managers) alimentent une **revue annuelle** du processus par la direction et le RSSI, dans une logique d'**amélioration continue du SMSI**.

3.1 Avant l'arrivée

La phase **"Avant l'arrivée"** correspond au pré-boarding sécurité du nouvel arrivant.
L'objectif est que, dès le Jour J, tout soit prêt pour qu'il puisse travailler dans de bonnes conditions, en respectant les exigences **sécurité** et **RGPD**, sans perte de temps pour les équipes.

- **Cadrage des accès** : le manager (N+1) définit les droits nécessaires selon le principe du moindre privilège, avec l'IT et le RSSI pour les outils sensibles et le télétravail.
- **Conformité RH / sécurité** : charte et clauses de confidentialité intégrées au dossier, fiche de risques métier, visite médicale si besoin.
- **Préparation technique** : création du compte SSO, activation MFA, rattachement aux bons groupes, droits dans M365/Google Workspace, Teams, Jira, GitLab, mise à disposition du PC, téléphone, VPN, authentificateur.
- **Parcours de formation** : affectation des e-learnings obligatoires (sécurité, RGPD, phishing, code de conduite) et planification des réunions d'onboarding (RH, IT, Sécurité, manager).
- **Accompagnement** : désignation d'un tuteur sécurité et clarification de son rôle.

À la fin de cette phase, **tous les prérequis sécurité** (comptes, équipements, formations, accompagnement) sont en place pour démarrer sereinement la suite du parcours.

3.2 Jour J → Semaine 1

La phase **Jour J → Semaine 1** marque le démarrage effectif du collaborateur.
Elle vise à le rendre **autonome**, à le **sensibiliser immédiatement à la sécurité** et à vérifier que tout ce qui a été préparé fonctionne correctement.

Actions clés :

- **Accueil RH** et remise des documents sécurité (livret, charte, fiche de risques).
- **Présentation sécurité** (manager/RSSI) : règles internes, mots de passe, phishing, partage de documents, RGPD, signalement d'incident.
- **Onboarding IT** : vérification du poste (chiffrement, antivirus, mises à jour, MFA) et des accès (SSO, Teams, SharePoint/Drive, Jira, GitLab, VPN).
- **Intégration métier** par le N+1 : rôle, responsabilités, données manipulées, confidentialité.
- **Réunions d'intégration** avec RH, IT, Sécurité et manager.
- **Lancement des e-learnings obligatoires** (sécurité, RGPD, phishing, code de conduite).
- **Suivi par le tuteur sécurité** sur les manipulations sensibles (partage, stockage, accès, signalement).
- **Contrôle initial des accès** par le manager (droits corrects, pas d'accès excessif).

3.3 Parcours 30/60/90 jours

Cette phase permet de **vérifier la bonne application des règles**, de **contrôler les accès dans la durée**, d'**accompagner la montée en compétence** et de **fournir des preuves de conformité** au **RGPD** et aux bonnes pratiques **ISO/IEC 27001**.

- **J+30 – Vérification initiale**
  - Revue des droits d'accès (moindre privilège).
  - Vérification de la réalisation des e-learnings obligatoires.
  - Point d'intégration N+1 / tuteur (retour d'expérience).
  - Mise à jour RH (ex. visite médicale).
- **J+60 – Approfondissement**
  - Revue des accès partagés (Teams, SharePoint/Drive, Jira, GitLab…).
  - Observation des pratiques de sécurité au quotidien.
  - Retour du tuteur sécurité (autonomie, besoins de formation).
- **J+90 – Validation finale**
  - Entretien de validation sécurité (bilan global).
  - Consolidation des preuves (attestations, charte, checklist, revue des accès).
  - Ajustement définitif des droits (suppression des accès inutiles).
  - Clôture du parcours : collaborateur autonome et conforme au SMSI.

3.4 Rôles et responsabilités

Le processus d'accueil en sécurité mobilise plusieurs acteurs : RH, Manager (N+1), IT, Équipe Sécurité/RSSI, Tuteur Sécurité et le collaborateur lui-même.
Afin d'assurer une exécution cohérente, sans doublon ni oubli, la répartition des responsabilités s'appuie sur un modèle **RACI** :

- **R = Responsable (exécute l'action)**
- **A = Accountable (rend des comptes / valide)**
- **C = Consulté (donne un avis / expertise)**
- **I = Informé (tient informé de l'avancement)**

Cette section présente une vue synthétique des missions principales de chaque rôle dans le processus. La répartition détaillée des responsabilités, formalisée selon le modèle RACI pour les étapes 3.1, 3.2 et 3.3, est fournie en annexe.

Rôle	Missions principales dans le processus
Manager (N+1)	Définit les accès, pilote le parcours 30/60/90 jours, réalise les entretiens et valide l'intégration sécurité.
RH	Gère le dossier administratif, clauses et charte, visite médicale, e-learnings et archivage des preuves.
IT	Crée et configure les comptes, MFA, équipements, droits aux outils collaboratifs et métiers, support technique.
Sécurité / RSSI	Cadre les exigences sécurité/RGPD, anime les sensibilisations, contrôle les accès et valide la conformité globale.
Tuteur sécurité	Accompagne le collaborateur au quotidien sur les usages, bonnes pratiques et remontée des risques
Collaborateur	Réalise les formations, applique les règles, signale les incidents et contribue à la culture sécurité.

4. Sensibilisation et conformité

Cette partie complète le processus d'accueil décrit en section 3 en détaillant les contenus de sensibilisation, la charte, la traçabilité et les exigences de conformité associées.

4.1 Contenus obligatoires + charte

La sensibilisation sécurité fait partie du parcours d'intégration dès la première semaine, afin de donner rapidement aux nouveaux arrivants les bons réflexes pour travailler en sécurité, sans entrer dans des détails trop techniques.

La séance d'accueil dure environ 30 minutes et se termine par un quiz de 15 minutes, ce qui permet de vérifier que les points essentiels sont compris.

Pour pouvoir prouver facilement que la formation a bien été suivie, on conserve trois éléments dans un dossier unique :

- la charte informatique signée,

- le score du quiz (objectif : 80 % ou plus),
- une preuve de présence à la session.

Le contenu abordé pendant la session d'accueil couvre notamment :

- les mots de passe : créer un mot de passe solide, éviter la réutilisation, utiliser la double vérification et un gestionnaire ;
- les e-mails suspects : vérifier l'adresse réelle de l'expéditeur, survoler les liens, ne pas ouvrir une pièce jointe douteuse, demander une confirmation en cas de doute ;
- le partage de fichiers : Vérifier les droits (lecture/édition) et éviter les clés USB ;
- le poste de travail : laisser les mises à jour actives, verrouiller son écran dès qu'on quitte son bureau;
- le télétravail : privilégier les outils de l'entreprise, éviter le Wi-Fi public, utiliser le partage de connexion si besoin.

➢ Charte d'utilisation des moyens informatiques

La charte informatique reprend les règles essentielles pour travailler dans de bonnes conditions et éviter les problèmes. Elle rappelle que les outils fournis par l'entreprise sont là pour le travail, et que chaque compte est personnel : on garde ses identifiants pour soi, sans les partager, même "pour dépanner".

Elle précise aussi qu'on ne doit installer que les logiciels validés par l'entreprise, histoire d'éviter des applications qui pourraient poser problème ou mettre en risque le poste.

Pour ce qui est des informations, la charte revient sur des réflexes du quotidien : verrouiller son écran quand on s'absente, ne pas laisser traîner de documents sensibles, garder un espace de travail rangé.

L'objectif est que tout soit clair pour tout le monde : ce qui est autorisé, ce qui ne l'est pas, et surtout comment chacun peut contribuer à garder un environnement de travail sécurisé au quotidien.

➢ Rôles et responsabilités

- RH : remet la charte et récupère la signature.
- Manager : vérifie que la formation est suivie la première semaine.
- Équipe informatique : prépare le poste, active les protections, explique les outils.
- Référent sécurité : anime la session, répond aux questions, suit les incidents.
- Nouvel arrivant : suit la formation, passe le quiz, signe la charte et applique les règles.

4.2 Traçabilité

Pour chaque nouvelle personne, nous gardons une trace simple de ce qui a été fait. L'idée est d'avoir, au même endroit, la charte signée, le résultat du quiz, la preuve de présence à la session, et la date de remise des supports.

Nous rangeons tout dans un dossier partagé : Onboarding sécurité/Année/Équipe/Nom_Prénom/. Pour s'y retrouver facilement, on applique une règle de nommage claire : Nom_Prénom_TypePreuve_YYYY-MM-DD.ext, exemples : Condette_Jeremy_Charte_2025-11-04.pdf.

Un tableau de suivi centralise l'essentiel, les colonnes sont simples : Nom, Équipe, Date d'arrivée, Session suivie (Oui/Non), Score au quiz, Charte signée (Oui/Non), Dossier complet (Oui/Non), Commentaires. Ce tableau sert de point de contrôle hebdomadaire.

Côté preuves, nous acceptons au choix : une feuille d'émargement signée, un export de la réunion en ligne, ou une capture d'écran claire. Pour le quiz, un export PDF/CSV ou une capture où figurent le nom, la date et le score suffit. Les dossiers restent accessibles en lecture à l'équipe concernée, et seuls les responsables de l'onboarding peuvent modifier les fichiers.

Enfin, quelques cas particuliers sont traités simplement. Si la session a été reportée (absence, maladie), une nouvelle date est fixée sous sept jours. Si le score au quiz est inférieur à 80 %, une seconde tentative est proposée dans les cinq jours.

4.3 Exigences de conformité (internes/contractuelles)

Dans notre contexte, Veridia doit prouver deux choses simples : d'un côté, que les règles internes sont bien appliquées par tous ; de l'autre, que les engagements pris dans les contrats clients sont respectés.

Exigences internes

L'entreprise formalise des règles claires À l'arrivée d'une nouvelle personne, on s'assure que :

- la charte d'utilisation est lue et signée ;
- la formation "accueil sécurité" est suivie dans la première semaine et validée par un quiz ;
- les accès sont ouverts "au juste besoin" et validés par le manager.
- une revue de ces accès est faite à J+30 pour retirer ce qui n'est pas utile.

Exigences contractuelles

Pour rester concrets, on couvre systématiquement :

- formation sécurité obligatoire pour toute personne ayant accès aux données d'un client ;

- retrait des accès le jour du départ
- protection des données : partage dans les outils de l'entreprise, droits d'accès.
- gestion des incidents : signalement rapide en interne (qui, quoi, quand, actions faites).

5. Outils et indicateurs

5.1 Outils / supports

Nous voulons former vite, avec des supports simples. La présentation d'accueil tient sur une dizaine de minutes (PowerPoint) et se termine par un quiz automatique (Google Forms) d'une vingtaine de questions. Les points clés sont résumés sur des fiches PDF d'une page (mots de passe, e-mails suspects, partage de fichiers). Un court message programmé chaque mois dans Teams rappelle un conseil et renvoie vers la fiche adaptée.

Pour préparer l'arrivée, on suit des étapes claires dans un outil de tâches (Jira) : une carte « Onboarding – Nom» contient des cases à cocher (compte créé, poste prêt, session planifiée, charte envoyée). Les accès sont validés par le manager via un petit tableau Excel.

5.2 Amélioration continue

Nous suivons peu d'indicateurs, lisibles en 30 secondes lors du point hebdomadaire. L'idée est d'identifier tout de suite ce qui manque et d'agir sans attendre.

Indicateurs de base:

- Taux de parcours terminé : session suivie + quiz validé + charte signée / nombre d'arrivants.
- Score moyen au quiz : moyenne des scores de la semaine.
- Dossiers complets : part des dossiers marqués « complet » dans le tableau de suivi.

Amélioration continue : en fin de mois, un retour d'expérience de 15 minutes recense ce qui a coincé (planning, message peu clair) et ce qui a bien marché. Nous mettons à jour si besoin une fiche ou la check-list.

6. Recommandations

- Planifier la session d'accueil sécurité avant l'arrivée et envoyer la charte à signer dans le mail d'accueil.
- Bloquer un créneau « Jour J » de 45 minutes : 10 min installation, 20 min présentation, 15 min quiz.
- Utiliser un modèle unique d'invitation (lieu/lien, documents à lire, contact en cas de souci).

- Tenir un tableau de suivi à jour chaque semaine et relancer immédiatement ce qui manque.
- Limiter les accès au « juste besoin » dès le départ et faire une mini-revue avec le manager à J+30.
- Mettre à jour le quiz et les fiches tous les 6 mois (numéro de version + date visibles).
- Former aussi les prestataires et alternants, avec les mêmes règles et les mêmes preuves.
- En cas d'incident signalé (mail suspect, perte de PC), remercier, corriger vite, puis partager le retour d'expérience à l'équipe.

7. Conclusions nominatives

BEN BEKKOU Lynda — Conclusion
Ce travail m'a montré qu'un bon accueil en sécurité repose surtout sur des règles simples et faciles à suivre. J'ai aussi compris l'importance d'organiser clairement qui fait quoi dès le début. Ça rend le processus plus fluide et évite beaucoup d'oublis.

IBEROUALENE Melissa — Conclusion

Travailler sur l'accueil en sécurité m'a surtout confirmé qu'on gagne avec du simple et du carré : SSO+MFA dès J1, accès au moindre privilège, MDM obligatoire, et des petites formations qui vont à l'essentiel. Ce qui change tout, c'est l'organisation : qui fait quoi, quand, et une trace propre dans Jira. Avec ça, on évite les ratés, on rassure les clients, et on peut prouver facilement que c'est fait.

CONDETTE Jérémy — Conclusion
En préparant la sensibilisation (contenus, fiches, quiz), j'ai vu que les messages concrets (mails piégés, partage de fichiers, verrouillage d'écran) marquent mieux que la théorie. Le vrai défi est la durée : dire l'important en 30 minutes et garder une trace propre.

KACED Inès — Conclusion
En travaillant sur les outils et les indicateurs, j'ai vu qu'un suivi simple suffit pour garder une vision claire de l'avancement. Le tableau de suivi aide vraiment à repérer ce qui manque. La seule limite reste sa mise à jour manuelle, qui mériterait d'être améliorée.

NIRERE Flavia — Conclusion
En rassemblant les recommandations, j'ai confirmé que la réussite tient surtout à l'organisation : invitation standard, créneau bloqué le Jour J, revue des accès à J+30 et relances rapides.

Références

Normes et cadres réglementaires

- ISO/IEC 27001 — Information Security Management Systems: Utilisé pour structurer le processus d'accueil
- ISO/IEC 27002 — Code of Practice for Information Security Controls: Référence des bonnes pratiques
- Règlement Général sur la Protection des Données (RGPD) — Appui réglementaire pour les risques et obligations

Onboarding

- **Slides du cours (Processus)**
- **unboarding**

Guides et bonnes pratiques

- ANSSI — https://cyber.gouv.fr/publications/guide-dhygiene-informatique
- https://cyber.gouv.fr

Charte informatique et sensibilisation

- https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/charte-dutilisation-des-moyens